

APPLICATION
FOR
UNITED STATES LETTERS PATENT

TITLE: USING BIOMETRICS AS AN ENCRYPTION KEY
APPLICANT: SCOTT C. HARRIS

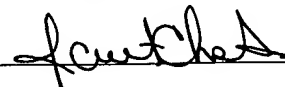
CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Label No. EL584933440US

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail Post Office to Addressee with sufficient postage on the date indicated below and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

May 24, 2000
Date of Deposit

Signature



Janet Christy
Typed or Printed Name of Person Signing Certificate

004250" 6442450

USING BIOMETRICS AS AN ENCRYPTION KEY

Background

5 Biometrics allows a person to use a unique part of their body for identification purposes.

Many different body part templates have been suggested for biometrics, including fingerprints, face prints, retinal scans and DNA sequences.

10 Many different ways of obtaining and using biometric information are well known in the art. The body part is compared with a prestored template. A match between the part and the template allows some action to be taken. Effectively these previous biometric systems used the biometric information as a
15 key that opens a lock. The biometric information is compared with a template. The lock opens based on the comparison.

Continuing the analogy, once the key has unlocked the lock, the user has access to information.

Encryption has also been used for security, but in a
20 different way. Encryption is used to change the information itself. No lock and key is necessary - the information can be disseminated, and the decryption key can be used to retrieve it.

Encryption is often used for messages, e.g. by email.
Encryption is also used to keep private certain information in an account, for example.

One popular kind of encryption is public key cryptography.

5 The encryption key is public and anyone can use it. Only the person having the private key can decrypt a message, however. If user A encrypts a message with user B's public key, only B can decrypt the message. No one else, not even user A, can decrypt the message. Other similar cryptosystems are known. All have in
10 common that there must be a decryption key - typically a large number.

Summary

15 It can be difficult to store the key for an encryption system. For instance, in a public key cryptography system, the user typically stores their private key inside their computer. However, a person with access to the user's computer can obtain access to the private key with much less security than is provided by the key itself. The private key is too long to
20 memorize (e.g. 128 bits), and instead must be transported for example on a transportable storage medium. This is by itself inconvenient.

The present application teaches a way of using biometrics to form an encryption and/or decryption key. The biometric information itself is translated into an encryption and/or decryption key. Therefore, the key is always available to the user, since it is formed based on the user's body parts.

The key is formed by comparing the relationship of parts of the biometric information.

An aspect of the invention uses a sequence of biometric information as the key. Only the specified sequence forms a proper key. Therefore, surreptitiously obtaining the user's biometric information will not enable forming a proper key without also knowing the proper combination.

Another aspect uses relative information from the biometric information to form the key. In this way, the key is formed independent of the absolute dimensions of the biometric information. The key that is formed can use the obtained information as a "seed", or can use the information directly.

Yet another aspect uses the concept of relative dimensions with biometrics as they have been conventionally been conceived, to determine if the biometric information fits a proper profile, and use that recognition to allow access.

Figure 1 shows an embodiment;

Figure 3 shows a flowchart of operation; and

Description of the Embodiments

In a particularly preferred embodiment, the security software 120 is a public key encryption/decryption system. The private key is based on the user's biometric information.

4

110, running the application program 120, for example, a security program.

004449-504400
5 The biometric device 102 can be any conventional fingerprint reader, which reads and produces an analog image or digital sample of the fingerprint. Either case produces what is effectively an image of the user's fingerprint. The image is conceptually shown in Figure 2. All fingerprints have certain general characteristics. The fingerprints have a number of ridges 222, 224, 226, which come together at a substantially center point 200. The center point of the user's fingerprint is taken as a center line. A number of ridges are formed around that center point. The lines on each user's fingerprint are different. A typical fingerprint may have approximately 25 to 35 lines in the width wise direction, and approximately 30 to 60 lines in the length wise direction. In this embodiment, the center point 200 is used as a point to draw reference lines. The reference line 210 defines a widthwise direction and the line 220 defines a lengthwise direction.

20 Since a typical fingerprint scanner provides an image of the entire fingerprint, all of this processing can be done in the computer 99. This is carried out according to the flowchart of Figure 3 which may run on computer 110.

At 300, the system finds a reference point and defines reference lines. The reference lines can include one line such as 210 in Figure 2, or alternatively can be more than one reference line. A second reference line, for example could be reference line 220 in Figure 2. Since the whole image of the fingerprint is available these lines can easily be made parallel or perpendicular to an "axis".

At 302, the system determines ridge spacing along the reference line. For example, in Figure 2, a first ridge 222 closest to the determined center is taken as the first found ridge. This is the ridge closest to the reference point, and avoids determination of the edge of the fingerprint, or determining what is the first ridge. The ridge 222 in this embodiment is defined as the ridge, on the left, closest to the center. The second ridge 224 is the next ridge over to the left.

The ridge 226 after that is the next ridge to the left. For purposes of illustration, the system determines the spacing between 10 ridges on the left and 10 ridges on the right. This produces 20 values.

At 304, the system finds the average of all the values.

Then at 306 the current value is compared to the average. "0" is defined if the current value is higher than the average,

or a "1" if the current value is lower than the average. If the spacing is equal to the average, then the value is taken as the inverse of the bit before it.

A simple example is shown in Figure 4. The sensor 100
5 detects distances, here shown as 5, 4, 6, 8, 9 and 4. The total
of these is 36, and since there are six distances, the average is
6. Now each of the values is compared with the average, to obtain
00X110, since the last bit represents a tie. This flips the x
bit before it to obtain 001110. At 308, the value thus obtained
10 is stored as part n of the key. 310 detects if the key is
complete. If so, the key is used at 312. If not, flow returns to
300 to obtain another part of the key. This can use another
specified reference line, e.g., a perpendicular line such as
shown as line 220. It could alternately and more preferably be
15 biometric information from a different biometric part, e.g. a
different finger.

The lines that are used to obtain the information can also
be at specified angles to the reference lines, e.g., at 22
degrees. The angles can be set, or can be entered by the user,
20 as a form of personal identification. For example, the user can
enter 22 while a specified finger is in the reader. This takes
the line along 22 degrees. It effectively forms a PIN that must

be entered to obtain the proper code from the biometric information.

By piecing together the decryption key from different body parts, the present system also provides an additional layer of security. The system above has described getting about 20 digits from a single biometric scan. This may correspond to 20 bits. If two orthogonal dimensions are defined as shown in the picture, this doubles the amount of information to 40 bits. However, by combining three fingerprints, a much more robust key length of 120 bits can be obtained. Moreover, additional security is provided by the specific selection of fingerprints. Only the user knows which biometric items to input, how many, and in which order. This effectively forms a barrier against others using this information.

An advantage of the present system comes from the use of relative, rather than absolute, information. No calibration is necessary, since each of the values is calculated based on comparing parts of the fingerprint to itself, not to some absolute reference. The digits are unambiguous, since there is no calibration, only an internal sensing of relationships among the different parts. The only necessary commonality is resolution -- the image sensor used must have sufficient

resolution to sense each ridge of the fingerprint.

Figure 4 shows an embodiment in which the fingerprint sensor is actually an image sensor chip, e.g., a CCD image sensor or active pixel sensor type device or infra-red photodetect. The chip's active surface is usually placed to receive the image of a larger area. However, in this embodiment, the pixels of the sensor are directly mapped to the user's finger. The finger is placed directly on the sensor. The position and orientation of the user's finger does not matter, since an unambiguous reference is obtained from the comparison of the different parts of the biometric information.

Another embodiment uses the relative relationship of the biometric information as described above in the conventional way that biometric information has been used. The relative relationship among the biometric information is used to form a number. That number is compared against a prestored number to determine identity. The test yields a pass if the information agrees.

Other biometric information can be used in a similar way. Retinal scans can be used by determining the same kind of relationship among lines of the scan, for example.

Other embodiments are within the disclosed invention.